

Applicant Initiated Interview Request Form

Application No.: 10/654,667 First Named Applicant: Kenneth Gould
 Examiner: Ryan Jakovac Art Unit: 2445 Status of Application: Non-Final

Tentative Participants:

(1) Elliott Light (2) _____
 (3) _____ (4) _____

Proposed Date of Interview: To be determine Proposed Time: _____ AM/PM

Type of Interview Requested:

(1) ☒ Telephonic (2) ☐ Personal (3) ☐ Video Conference

Exhibit To Be Shown or Demonstrated: ☐ YES ☒ NO

If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) <u>Rejection</u>	<u>claim 18</u>	<u>Jones</u>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2) _____	_____	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3) _____	_____	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4) _____	_____	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Continuation Sheet Attached


Brief Description of Argument to be Presented:

See attached for discussion of arguments.

An interview was conducted on the above-identified application on _____.

NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.


 Applicant/Applicant's Representative Signature
Elliott D. Light
 Typed/Printed Name of Applicant or Representative
51948

 Examiner/SPE Signature

 Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Appl. No. 10/654,667

Response to Office Action Mailed February 25, 2009

VIA FACSIMILE – 571-270-6003

From: Elliott Light (Contact: e-mail – elight@globe-ip.com; telephone: 703.391.2900)
To: Examiner Ryan Jakovac
Subject: Talking Points for Telephonic Interview (TO BE SCHEDULED)

Attorney Docket No.: 2816-026

Application Serial No.: 10/654,667

This paper responds to the office action mailed February 25, 2009.

GENERALLY

- Claims 18, 19, 21, 23-26, 28 and 30-35 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication 2007/0214083 filed by Jones et al. in view of U.S. Patent Application Publication 2001/0044818 filed by Liang (hereinafter, "Liang"). Claims 20 and 27 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Jones. Claims 22 and 29 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Liang and in further view of U.S. Patent Application Publication 2004/0006621 filed by Bellison et al. (hereinafter, Bellison).

REJECTIONS UNDER §103(a)

- Claim 18 as proposed for amendment recites the following limitations:
 - 18. (Proposed) A system for providing data filtering from a cable modem termination system (CMTS) in a cable data network comprising:
 - the CMTS, wherein the CMTS comprises a first network interface, a second network interface, a data gateway agent, and wherein the CMTS is configured for obtaining a packet count from a packet counter, wherein the packet count is determined from ~~at least one of a downstream packet count indicative of downstream packets received via the first network interface and sent to a subscriber device via the second network interface and an upstream packet count indicative of the packets received from the subscriber device via the second network interface for transmission via the first network interface;~~ and
 - a datastore accessible to the data gateway agent for storing a selected data transfer rule, wherein the selected data transfer rule comprises URL downstream filtering criteria selected by a subscriber, and
 - wherein the data gateway agent receives the downstream packets via the first network interface prior to receipt of the downstream packets by the packet counter, accesses the datastore, uses the URL-filtering criteria to make a filtering determination with respect to the downstream packet~~packets~~, wherein the filtering determination is selected from the group consisting of allowed and blocked, and if ~~the a downstream~~ packet is allowed, then forwards the downstream packet to the packet counter for counting, and if the downstream packet is blocked then applies a corrective measure to the downstream packet.

Appl. No. 10/654,667

Response to Office Action Mailed February 25, 2009

- Independent claim 18 is drawn to a system for providing a downstream data filter at a CMTS. The filtering is performed before downstream packets arrive at a downstream counter in the CMTS, so that packets that are not desired by a subscriber are not sent to the subscriber and counted against a subscriber limit. The filtering is performed by application of a downstream data transfer rule comprising packet content criteria selected by the subscriber.
- Jones generally describes a system and method for providing prepaid data service. A subscriber pre-pays for services by creating a credit in an account. As the subscriber utilizes various services, the account is debited. When the account reaches a threshold, the subscriber's access to services is terminated, and the subscriber is directed to a website to add additional value to the account. A pre-paid account may be purchased for various services. A service may be defined by network parameters (data rate, packet count), by service (e-mail, FTP), or by application (stock quotes, songs). A subscriber may define a service by disallowing certain protocols (See, Jones ¶[0058]).
- Applicant submits that Jones describes measuring account usage based on network access without regard to whether the access was initiated by a subscriber. While Jones may limit a subscriber's ability to access a network in the upstream direction, it does not teach filtering packets that are directed to a subscriber device in the downstream direction, particularly packets that are directed to the subscriber device that are not in response to a session initiation packet.
- Jones describes various policy enforcement mechanisms that monitor service usage and provide counts against a pre-paid credit.
- At paragraphs 0060-61, Jones describes a policy that is directed to counting packets, files, or other measures of usage. These policies are used for the benefit of the service provider to enforce a prepaid subscription service.

[0060] If the user of the subscriber terminal 12 has a prepaid account, the subscriber terminal 12 may display the screen of FIG. 4. FIG. 4 is an exemplary screen illustrating exemplary classes of prepaid data services selectable by the user of the subscriber terminal 12. The prepaid data services offered by the self-service portal may include timed access (e.g., 20 minutes of access) to the network or rate-controlled data access (e.g., 150 kbps) to the network. Other examples are peak or sustained data rate. The self-service portal may also offer service packages. The service packages may offer varying data rate services depending on the type of traffic. For example, HTTP traffic may be passed through the data gateway at a rate of 150 kbps, file transfer protocol (FTP) traffic may be passed at rate of 100 kbps, and video traffic may be passed at a rate of 250 kbps. The data rates may be selected based on delay sensitivities of the various types of traffic and the capabilities of the subscriber terminal 12.

[0061] Still alternatively, the web server 26 may offer various application layer services. The services may include transfer of a specific number of files (e.g., according to FTP) between the subscriber terminal 12 and the data network 20, transmission of a certain number of packets, download of a specific type of

Appl. No. 10/654,667

Response to Office Action Mailed February 25, 2009

content (e.g., a song), and/or performance of a specific type of transaction (e.g., a stock quote). Of course, other types of services are also possible.

- The services determine how a subscriber may access a network. The disclosures do not teach or suggest how a subscriber might avoid being charged for a packet that the subscriber does not want or did not initiate.
- Paragraph 0072 of Jones (cited in the Office Action) reads as follows:

[0072] The policy may also instruct the policy enforcement point to monitor the service granted to the subscriber terminal 12. For example, if the policy enforcement point is the PDSN 46 or switch 50, the policy may instruct the PDSN 46 or switch 50 to count the number of file transfers completed, the number of packets transmitted or received, the number of downloads of a song, and/or the number of stock transaction. At specific instants of time, the policy may also instruct the PDSN 46 or switch 50 to push the current count to the policy decision point 24. As each packet or transaction, for example, may translate into a number of utils, the policy decision point 24 may then adjust the balance of the prepaid account in accordance with the count.
- Paragraph 0072 describes enforcing a policy enforcement point but does not disclose how this enforcement is accomplished. As described, packets that are received are counted without regard to whether the packets are desired by the subscriber.
- Liang describes system and method for identifying and blocking unacceptable web content. The system comprises a proxy server connected between a client and the Internet that checks a requested URL against a block list that may include URLs identified by a web spider. If the URL is not on the block list, the proxy server requests the web content. When the web content is received, the proxy server evaluates the content for prohibited content. The proxy server may either block the retrieved web content or permit user access to it.
- The filtering of Liang operates on URLs or web content that is requested by a subscriber. Liang does not teach or suggest detecting a packet that is directed to a subscriber device outside of a session initiated by the subscriber.
- Based on the foregoing, Applicant respectfully submits that the combination of Jones and Liang does not anticipate claim 18 as proposed for amendment.